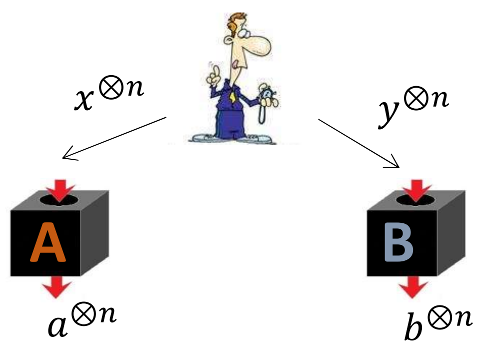
Concluding remark

- Note that there is a natural isomorphism between states of n pairs of qubits and states of a single pair of qu-Dits, for $D = 2^n$.
- If we are able to self-test $|\psi\rangle = \bigotimes_{i=1}^{n} \left(\cos\theta_i |00\rangle + \sin\theta_i |11\rangle \right)$, then we can also self-test some state of a single pair of qu-Dits.
- Hence, as a corollary of our result, we deduce that we can self-test an n dimensional subfamily of the family of all partially entangled states of two qu-Dits, for $D = 2^n$.
- With a different approach, C. & Goh & Scarani show that all pure bipartite entangled states can be self-tested[8].

THANK YOU!

[8] A. Coladangelo, K. T. Goh and V. Scarani (2016). All pure bipartite entangled states can be self-tested.

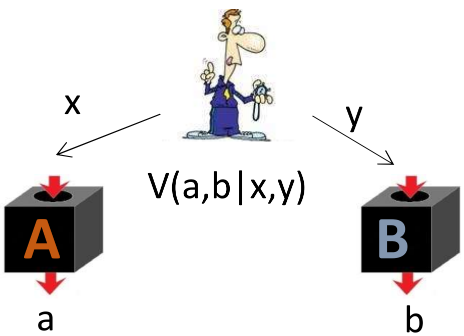
Rigidity of The Parallel Repeated Magic Square Game



$V(a^{\otimes n}, b^{\otimes n} | \, x^{\otimes n} \, y^{\otimes n})$

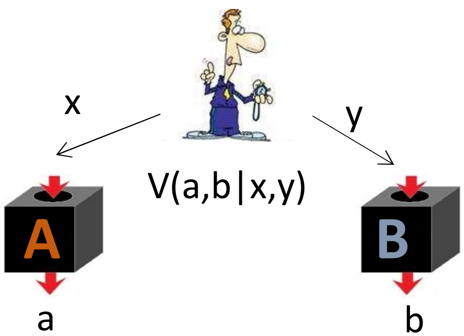
Matthew Coudron, Anand Natarajan
MIT EECS/CSAIL, MIT CTP

QIP '17



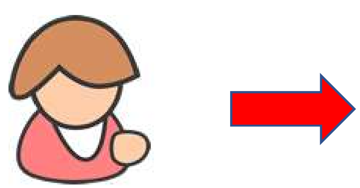
The Magic Square Game

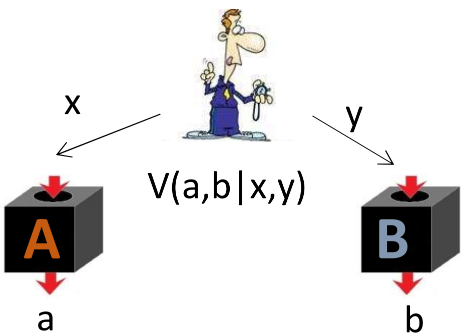
	Column 1	Column 2	Column3
Row 1			
Row 2			
Row3			



The Magic Square Game

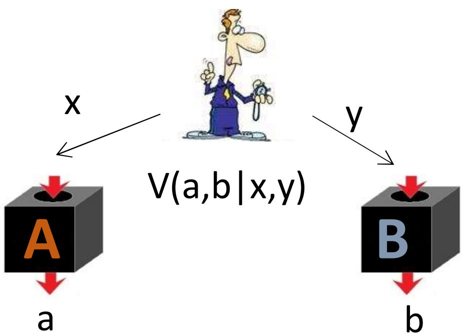
	Column 1	Column 2	Column3
Row 1			
Row 2			
Row3			



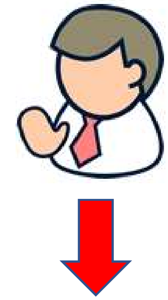


The Magic Square Game

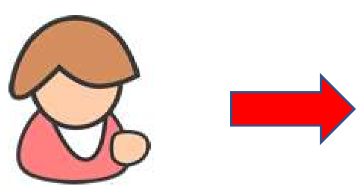
	Column 1	Column 2	Column3
Row 1			
Row 2			
Row3			

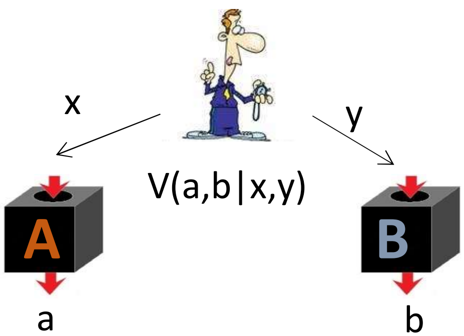


The Magic Square Game

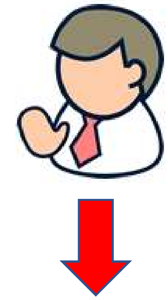


	Column 1	Column 2	Column3
Row 1			
Row 2			
Row3	1	1	-1

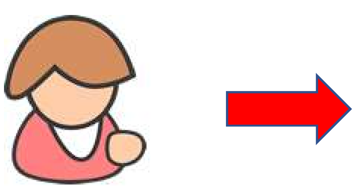


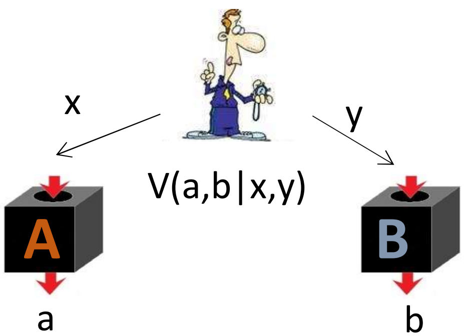


The Magic Square Game

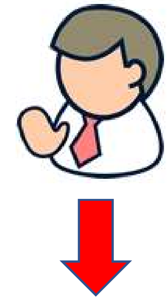


	Column 1	Column 2	Column3
Row 1			-1
Row 2			1
Row3	1	1	-1

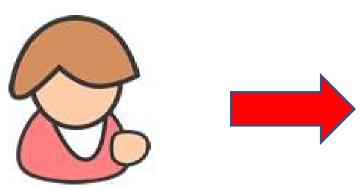




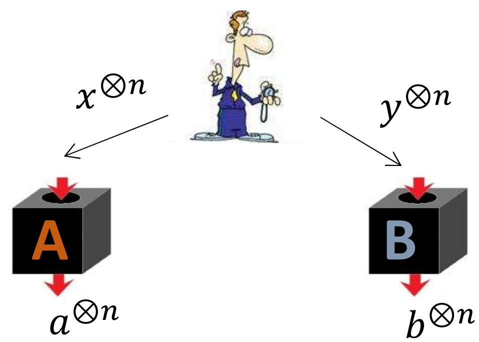
The Magic Square Game: The Ideal Strategy



	Column 1	Column 2	Column3
Row 1	$I \otimes \sigma_Z$	$\sigma_Z \otimes I$	$-\sigma_Z \otimes \sigma_Z$
Row 2	$\sigma_X \otimes I$	$I \otimes \sigma_X$	$-\sigma_X \otimes \sigma_X$
Row3	$\sigma_X \otimes \sigma_Z$	$\sigma_Z \otimes \sigma_X$	$-\sigma_Y \otimes \sigma_Y$



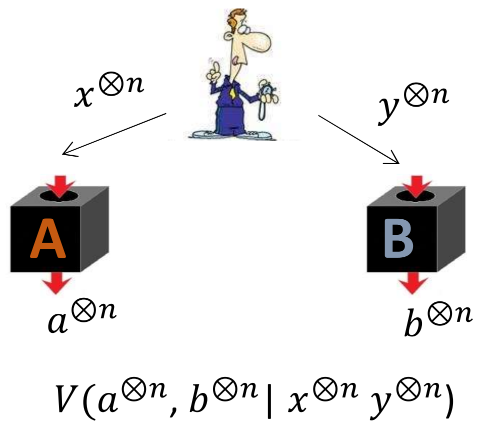
Main Theorem



$$V(a^{\otimes n}, b^{\otimes n} \mid x^{\otimes n}\, y^{\otimes n})$$

Rigidity of the n-round parallel repetition of the Magic Square game:

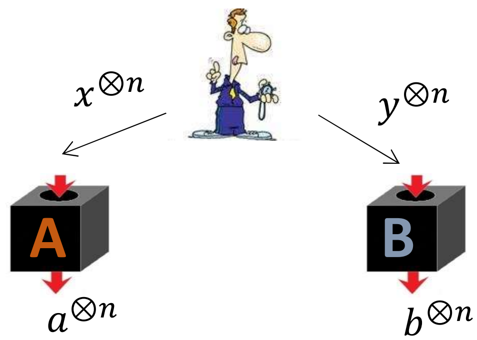
Main Theorem



Rigidity of the n-round parallel repetition of the Magic Square game:

- For any entangled strategy succeeding with probability 1 − ε, the players' shared state is O(poly(nε))-close to 2n EPR pairs under a local isometry.

Main Theorem



$V(a^{\otimes n}, b^{\otimes n} | x^{\otimes n} y^{\otimes n})$

Rigidity of the n-round parallel repetition of the Magic Square game:

- For any entangled strategy succeeding with probability 1 − ε, the players' shared state is O(poly(nε))-close to 2n EPR pairs under a local isometry.
- Furthermore, under local isometry, the players' measurements must be O(poly(nε))-close to the "ideal" measurements when acting on the shared state.

Motivation

Rigidity Theorems and self-testing results are a critical component of many results in Quantum Information:

Motivation

Rigidity Theorems and self-testing results are a critical component of many results in Quantum Information:

- Device independent protocols: QKD and randomness expansion ([VV12, CY13])

Motivation

Rigidity Theorems and self-testing results are a critical component of many results in Quantum Information:

- Device independent protocols: QKD and randomness expansion ([VV12, CY13])
- Interactive proofs for the local Hamiltonian problem ([FV14, NV16])

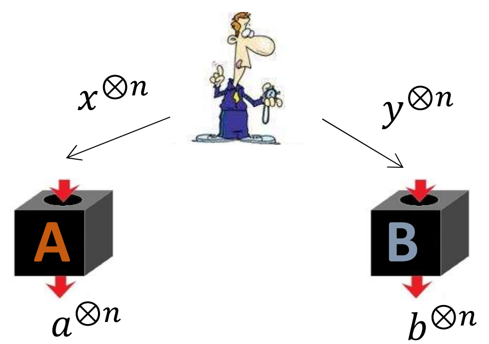
Motivation

Rigidity Theorems and self-testing results are a critical component of many results in Quantum Information:

- Device independent protocols: QKD and randomness expansion ([VV12, CY13])
- Interactive proofs for the local Hamiltonian problem ([FV14, NV16])
- Delegating Quantum Computation for a classical verifier ([RUV12, NV16])

Background and Intuition

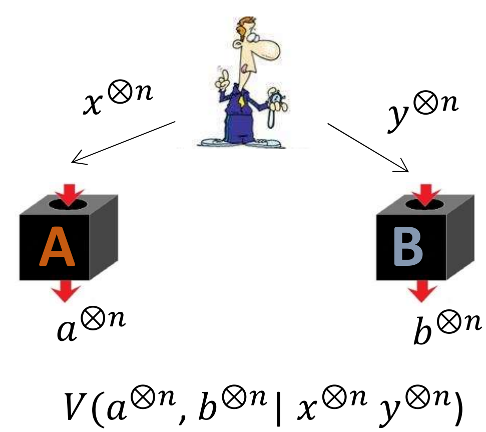
- Self-testing results for large games established in by McKague [McK15- "Self-testing in Parallel"]



$V(a^{\otimes n}, b^{\otimes n} | \, x^{\otimes n} \, y^{\otimes n})$

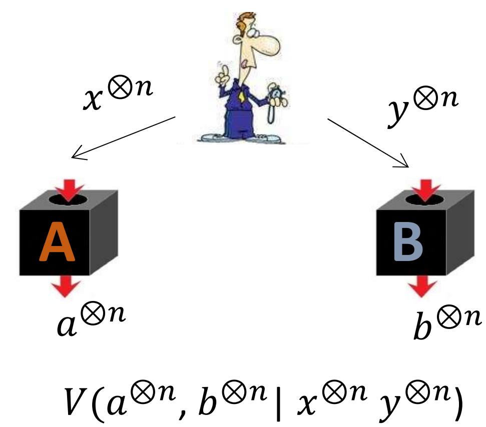
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  - Gives a self-test for n EPR pairs, with polynomial error dependence



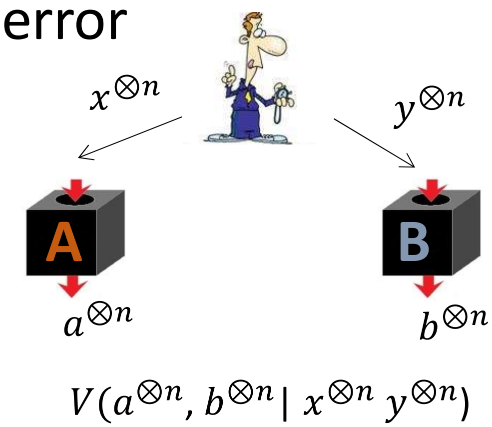
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  - Gives a self-test for n EPR pairs, with polynomial error dependence
  - Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence



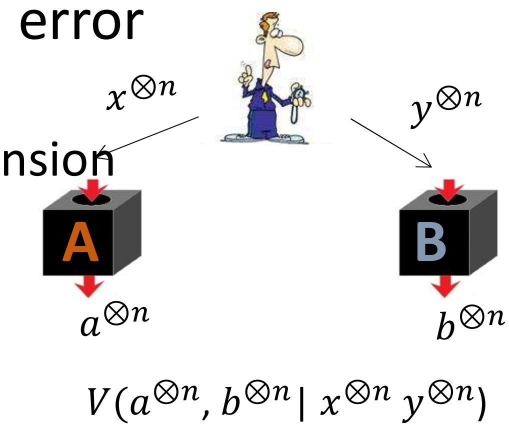
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  - Gives a self-test for n EPR pairs, with polynomial error dependence
  - Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence
- Improvement of classical verifier result to polynomial error dependence is prerequisite for applications in:



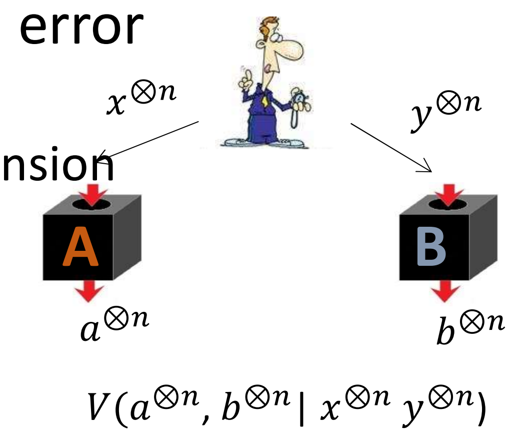
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  - Gives a self-test for n EPR pairs, with polynomial error dependence
  - Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence
- Improvement of classical verifier result to polynomial error dependence is prerequisite for applications in:
  - Device independent protocols: QKD and randomness expansion



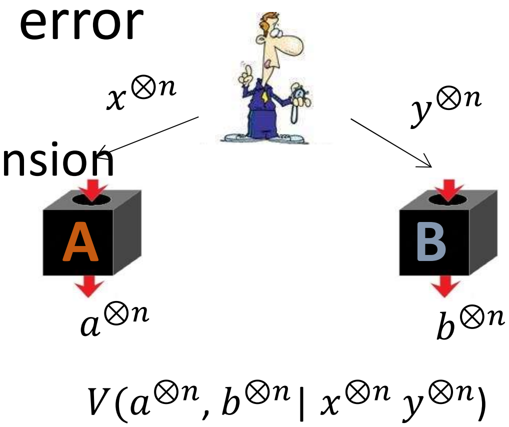
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  - Gives a self-test for n EPR pairs, with polynomial error dependence
  - Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence
- Improvement of classical verifier result to polynomial error dependence is prerequisite for applications in:
  - Device independent protocols: QKD and randomness expansion
  - Interactive proofs for the local Hamiltonian problem



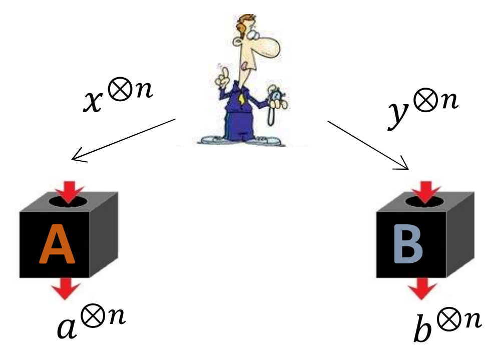
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- "Self-testing in Parallel"]
  - Gives a self-test for n EPR pairs, with polynomial error dependence
  - Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence
- Improvement of classical verifier result to polynomial error dependence is prerequisite for applications in:
  - Device independent protocols: QKD and randomness expansion
  - Interactive proofs for the local Hamiltonian problem
  - Delegating Quantum Computation for a classical verifier



Proof Structure

Theorem A: Commutation and Anti-Commutation

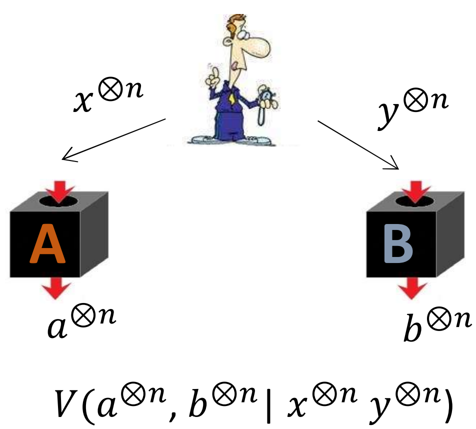


$V(a^{\otimes n}, b^{\otimes n} | x^{\otimes n}\, y^{\otimes n})$

Proof Structure

Theorem A: Commutation and Anti-Commutation

There exists a method for assembling Alice's projectors into unitaries $\tilde{A}^c_{r,k}$ (resp. $\tilde{B}^c_{r,k}$), for $k \in [n]$ such that:



Proof Structure

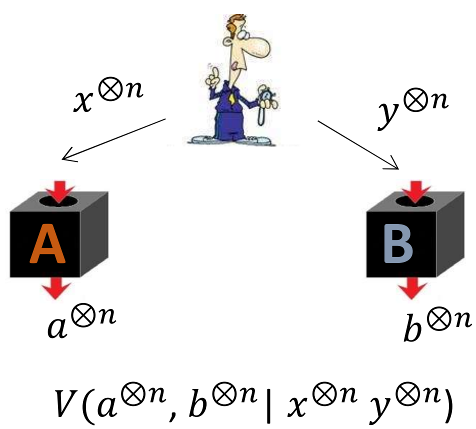
Theorem A: Commutation and Anti-Commutation

There exists a method for assembling Alice's projectors into unitaries $\tilde{A}^c_{r,k}$ (resp. $\tilde{B}^c_{r,k}$), for $k \in [n]$ such that:

$$d_{\psi'}(\tilde{A}^c_{r,k}\tilde{A}^{c'}_{r',k}, (-1)^{f(r,r',c,c')}\tilde{A}^{c'}_{r',k}\tilde{A}^c_{r,k}) \leq O(\sqrt{\epsilon})$$

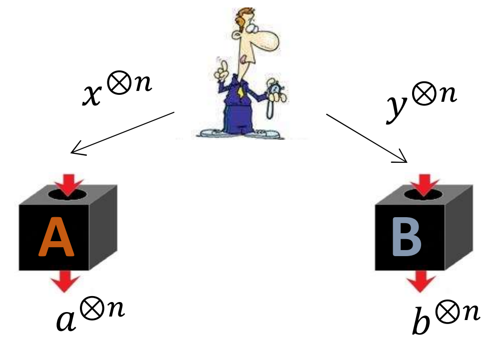
and

$$d_{\psi'}(\tilde{A}^c_{r,k}\tilde{A}^{c'}_{r',k'}, \tilde{A}^{c'}_{r',k'}\tilde{A}^c_{r,k}) \leq O(\sqrt{\epsilon})$$



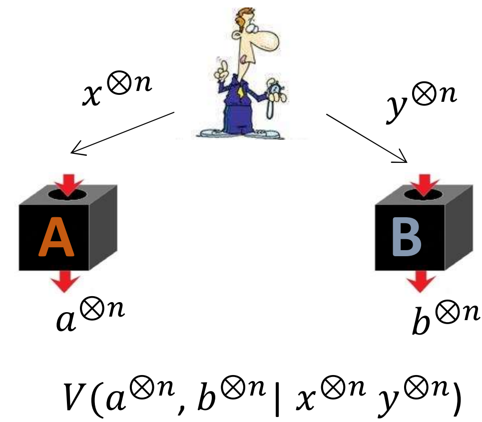
Proof Structure

Theorem B: The Isometry



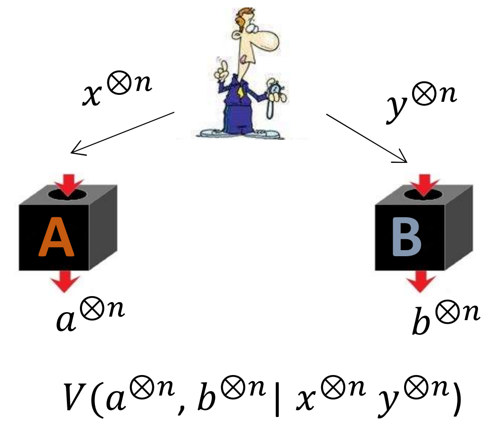
$V(a^{\otimes n}, b^{\otimes n} | \, x^{\otimes n} \, y^{\otimes n})$

Proof Structure



Theorem B: The Isometry

- There exist unitary operators ${W^A}_{\mathbf{s},\mathbf{t}}, {W^B}_{\mathbf{u},\mathbf{v}}$ constructed from the $\tilde{A}^c_{r,k}$ and $\tilde{B}^c_{r,k}$ respectively



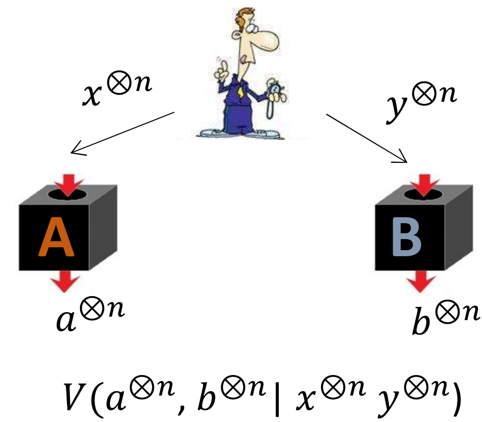
Proof Structure

Theorem B: The Isometry

- There exist unitary operators ${W^A}_{\mathbf{s},\mathbf{t}}, {W^B}_{\mathbf{u},\mathbf{v}}$ constructed from the $\tilde{A}^c_{r,k}$ and $\tilde{B}^c_{r,k}$ respectively
- And, there exists and isometry $V : \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n}$ and $|\phi\rangle \equiv V(|\psi\rangle)$ such that:

$$\left| \langle \phi | \sigma^A_X(\mathbf{s}) \sigma^A_Z(\mathbf{t}) \sigma^B_X(\mathbf{u}) \sigma^B_Z(\mathbf{v}) | \phi \rangle - \langle \psi | {W^A}_{\mathbf{s},\mathbf{t}} {W^B}_{\mathbf{u},\mathbf{v}} | \psi \rangle \right| \leq O(n^2 \sqrt{\varepsilon}),$$

Proof Structure



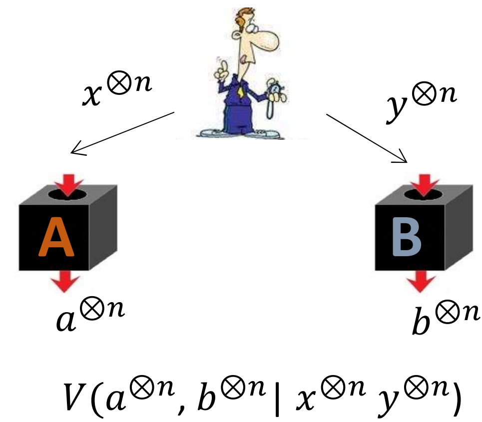
Theorem B: The Isometry

- There exist unitary operators ${W^A}_{\mathbf{s},\mathbf{t}}, \, {W^B}_{\mathbf{u},\mathbf{v}}$ constructed from the $\tilde{A}^c_{r,k}$ and $\tilde{B}^c_{r,k}$ respectively
- And, there exists and isometry $V : \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n}$ and $|\phi\rangle \equiv V(|\psi\rangle)$ such that:

$$\left| \langle \phi | \sigma_X^A(\mathbf{s}) \sigma_Z^A(\mathbf{t}) \sigma_X^B(\mathbf{u}) \sigma_Z^B(\mathbf{v}) | \phi \rangle - \langle \psi | {W^A}_{\mathbf{s},\mathbf{t}} {W^B}_{\mathbf{u},\mathbf{v}} | \psi \rangle \right| \leq O(n^2 \sqrt{\varepsilon}),$$

- This type of isometry was pioneered in works of McKague [McKague16], [Wu, Bancal, McKague, Scarani 16]

Proof Structure



Theorem B: The Isometry

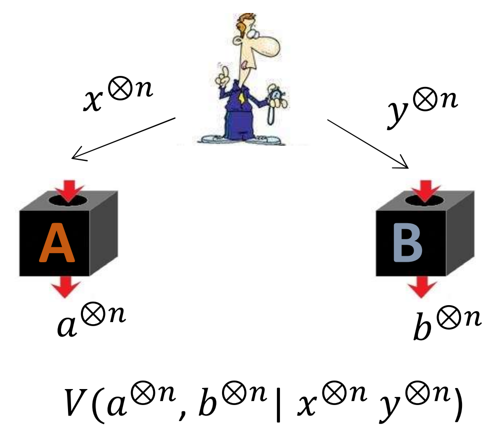
- There exist unitary operators $W^A{}_{\mathbf{s},\mathbf{t}}, W^B{}_{\mathbf{u},\mathbf{v}}$ constructed from the $\tilde{A}^c_{r,k}$ and $\tilde{B}^c_{r,k}$ respectively
- And, there exists and isometry $V : \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n}$ and $|\phi\rangle \equiv V(|\psi\rangle)$ such that:

$$\left|\langle\phi|\sigma_X^A(\mathbf{s})\sigma_Z^A(\mathbf{t})\sigma_X^B(\mathbf{u})\sigma_Z^B(\mathbf{v})|\phi\rangle - \langle\psi|W^A{}_{\mathbf{s},\mathbf{t}}W^B{}_{\mathbf{u},\mathbf{v}}|\psi\rangle\right| \leq O(n^2\sqrt{\varepsilon}),$$

- This type of isometry was pioneered in works of McKague [McKague16], [Wu, Bancal, McKague, Scarani 16]
- This theorem overlaps with [Chao, Reichardt, Sutherland, Vidick 16]

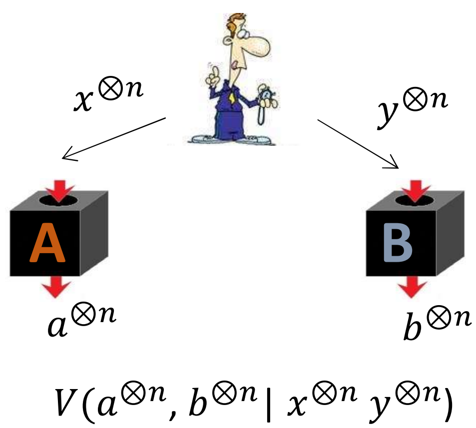
Conclusion

- Rigidity theorem for the parallel repeated magic square game which:



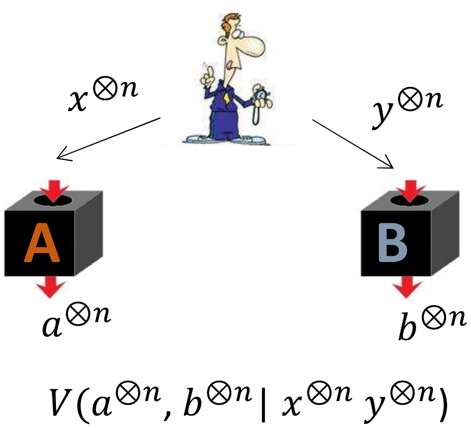
Conclusion

- Rigidity theorem for the parallel repeated magic square game which:
  - Self-tests n EPR pairs with polynomial error dependence



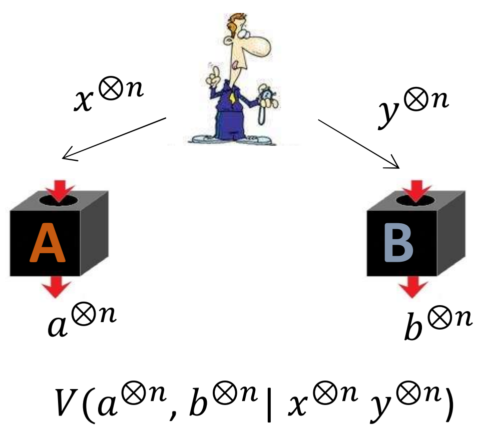
Conclusion

- Rigidity theorem for the parallel repeated magic square game which:
  - Self-tests n EPR pairs with polynomial error dependence
  - Certifies Pauli-product measurements with polynomial error dependence



Conclusion

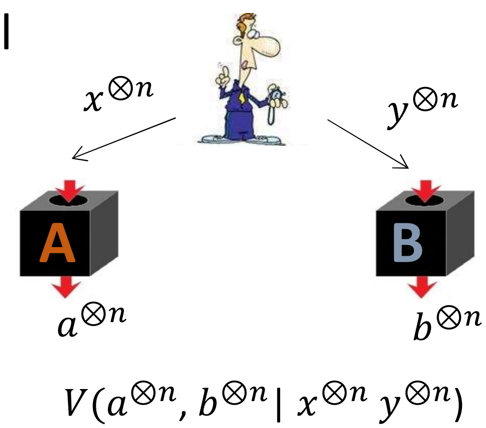
- Rigidity theorem for the parallel repeated magic square game which:
  - Self-tests n EPR pairs with polynomial error dependence
  - Certifies Pauli-product measurements with polynomial error dependence



- Open Problems:

Conclusion

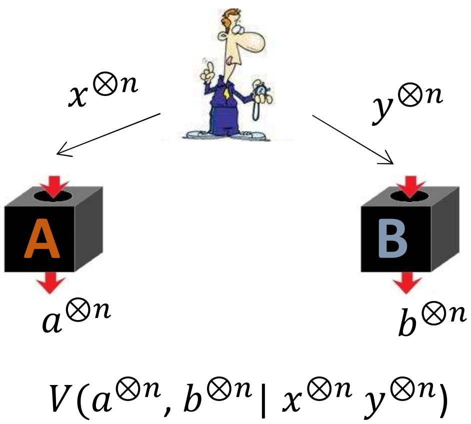
- Rigidity theorem for the parallel repeated magic square game which:
  - Self-tests n EPR pairs with polynomial error dependence
  - Certifies Pauli-product measurements with polynomial error dependence



- Open Problems:
  - Reduce error dependence – [NV16]

Conclusion

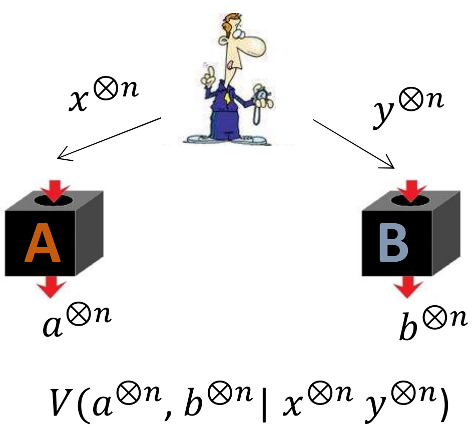
- Rigidity theorem for the parallel repeated magic square game which:
  - Self-tests n EPR pairs with polynomial error dependence
  - Certifies Pauli-product measurements with polynomial error dependence



- Open Problems:
  - Reduce error dependence – [NV16]
  - Reduce input size –[CRSV16]

Conclusion

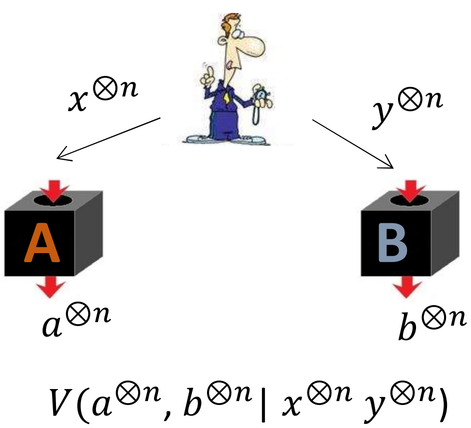
- Rigidity theorem for the parallel repeated magic square game which:
  - Self-tests n EPR pairs with polynomial error dependence
  - Certifies Pauli-product measurements with polynomial error dependence



- Open Problems:
  - Reduce error dependence – [NV16]
  - Reduce input size –[CRSV16]
  - Do both at the same time --- OPEN

Conclusion

- Rigidity theorem for the parallel repeated magic square game which:
  - Self-tests n EPR pairs with polynomial error dependence
  - Certifies Pauli-product measurements with polynomial error dependence



- Open Problems:
  - Reduce error dependence – [NV16]
  - Reduce input size –[CRSV16]
  - Do both at the same time --- OPEN
  - More applications to delegated quantum computation or interactive proofs for local Hamiltonian, randomness expansion.